REMARKS

The Examiner has rejected Claims 1-22 under 35 U.S.C. §102(e) as allegedly being anticipated by Segal (6,345,299). Applicant respectfully disagrees with such rejection.

Specifically, the Examiner relies on the following excerpt from Segal to make a prior art showing of applicant's claimed "maintaining a set of criteria for determining when one of said communications may be scanned at a computer node connected to the firewall instead of at the firewall" (see Claims 1 and 17), "maintaining a set of scanning rules for determining when a communication received at a firewall is to be scanned on the firewall and when said communication may be scanned by the destination node of said communication" (see Claim 7), "a set of criteria to be applied to said communication to determine if said communication is to be scanned for target content at the firewall or at the destination node" (see Claim 18), and "a set of rules configured to determine whether said communication is to be scanned for said target content on said firewall or on the first node" (see Claim 19).

> "In accordance with the invention, the network 40 the units 43, 45, 46, 47, 49, and 50 each comprise a shared list setting forth a plurality of listed nodes and a set of access privileges for each listed node. Access privileges are the types of transmissions that a given node listed in the shared list is permitted to make. For example, consider the case where node B1 is a computer or LAN at an accounting firm. The firm may want to restrict the nodes from which it receives or transmits E-mail or certain types of transmissions (i.e. File Transfer Protocol (FTP). In this case, the firm wishes to receive e-mail only form its clients Z1, Y2, and X4. Node B1 would instruct node 45 to provide that the shared list residing at security node 45 would intercept all e-mail and only allow e-mail form nodes Z1, Y2 and X4 but in this distributed system, it is also possible for security node 49 to only allow e-mail from Y2, node 50 prohibits e-mail form Z2 and so forth. Thus, with the cooperation of other nodes, it is virtually impossible to overwhelm node 45 with unpermitted transmissions. The shared list may provide with respect to any listed node that it can only transmit to certain other listed nodes and, with respect to those nodes it can transmit to, restrictions applicable to such transmissions." (col. 2, line 60 - col. 3, line 15)

The foregoing excerpt, however, simply makes the suggestion of the use of a "black list"-type feature whereby lists are used to determined which nodes are permitted to communicate with which nodes. In sharp contrast, applicant teaches and claims "maintaining a set of criteria for determining when one of said communications may be scanned at a computer node connected to the firewall instead of at the firewall" [or similar, but different, language (see above)]. Emphasis is added. This "scanning" of content or the like is different from Segal's filtering of origin nodes, etc.

Further, the Examiner relies on col. 3, lines 35-45 to make a prior art showing of applicant's claimed "virus" scanning. See Claim 7, in particular. However, such excerpt merely suggests lists of which nodes, sources, networks are allowed to use certain destinations. These commands are taught to be utilized by filtering devices and/or security devices such as firewalls, ingress nodes, switches, which would be informed which destination nodes, addresses, ports, are permitted to which source nodes or networks. This is very different from applicant's claimed virus scanning.

More importantly, the Examiner has apparently not taken into consideration another very important claimed feature that distinguishes the claimed invention from Segal. Specifically, applicant teaches and claims "maintaining a set of criteria for determining when one of said communications may be scanned at a computer node connected to the firewall instead of at the firewall" [or similar, but different, language (see above)]. Emphasis is added.

It is clear from the excerpt from Segal and the remaining reference that Segal merely discloses that "[t]he system presented allows for inter-firewall cooperation and sharing the load between various filtering and security devices. This provides for a distributed firewall capability and also permits (multiple) smaller firewalls and/or admission control points" (see col. 4, lines 20-25). In sharp contrast, applicant teaches and claims sharing the load between a firewall and "a computer node" where the content-containing communication is destined. Only applicant

teaches and claims such a load sharing capability that is specifically designed to share a "scanning" load among a firewall and "a computer node." See Fig. 1A.

Still yet, it is noted that Segal fails to show any particular criteria or rules that govern the manner in which the "scanning" is shared among a firewall and "a computer node." For example, with respect to Claim 1, applicant teaches and claims "maintaining a set of criteria for determining when one of said communications may be scanned at a computer node connected to the firewall instead of at the firewall."

The Examiner is reminded that a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. Of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Moreover, the identical invention must be shown in as complete detail as contained in the claim. *Richardson v. Suzuki Motor Co.*868 F.2d 1226, 1236, 9USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be arranged as required by the claim. This criteria has simply not been met by the Segal reference.

Yet further distinguishing the foregoing feature is applicant's dependently claimed subject matter which apparently has not been fully considered by the Examiner. Just by way of example, the Examiner relies on the foregoing excerpts from Segal to make a prior art showing of applicant's claimed:

"wherein said partitioning comprises:

receiving scanning capabilities of a first computer node connected to the firewall;

consulting a set of scanning requirements specified by an operator of the firewall; and

specifying a set of criteria to identify when a communication may be scanned for target content by said first computer node" (see Claim 4), and

"wherein said determining comprises:

identifying whether said firewall is capable of scanning said first communication for target content;

determining whether said firewall is configured to share responsibility for scanning said communications with one or more of said plurality of computer nodes;

determining whether said first node is capable of scanning said first communication for said target content; and

determining whether said communication satisfies one or more criteria in said set of criteria" (see Claim 6).

By virtue of the previous arguments, the present limitations have simply not been met by Segal since they provide additional limitations associated with applicant's claimed "maintaining a set of criteria for determining when one of said communications may be scanned at a computer node connected to the firewall instead of at the firewall." A specific prior art showing of such features or a notice of allowance is respectfully requested.

All of the Examiner's rejections and objections are thus deemed to be overcome, and a notice of allowance is respectfully requested.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. If any fees are due in connection with the filing of this paper, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1351 (Order No. NAI1P263/99.010.01).

Respectfully submitted,

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172
Telephone: (408) 505-5100